IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF TEXAS

TYLER DIVISION

THE PACID GROUP, LLC **Plaintiff,** **v.** **APPLE, INC., et al.,** **Defendants.**	**Civil Action No. 6:09-cv-143-LED**

PLAINTIFF'S OPENING BRIEF REGARDING CLAIM CONSTRUCTION

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page No

Cases

Statutes

Other Authorities

I. BACKGROUND AND NATURE OF CASE

The present case involves United States Patent Nos. 5,963,646 ("'646 Patent") (Ex. A)[1] and 6,049,612 ("the '612 Patent") (Ex. B) (collectively, "the Patents-in-Suit") owned by The PACid Group, LLC ("PACid"). PACid is a Texas limited liability company, owned, and operated by its managing member, Guy L. Fielder. (Lee Decl. Ex. C (Doc. No. 201-4); Fielder Decl. (Doc. No. 219-2).) Mr. Fielder is the first named inventor of the patents in suit. In addition to his technical prowess, Mr. Fielder has excelled in business and management. His decades-long career includes work at Texas Instruments and Compaq Computer Corporation, where he was one of Compaq's very first employees and eventually spearheaded the development of Portable Computers, contributing $2 billion in revenue to Compaq's bottom line and garnering awards like Portable Computer of the Year and Best PC Product of the Year. (*Id.*, ¶6; *id.*, Ex. A (Doc. No. 219-3) at 4.) Mr. Fielder has recently been the Chief Operating Officer of Celevoke, Inc., a subsidiary of Current Technology Corporation, anticipated to become a market leader in the projected $38.3 billion (by 2011) global market for Telematics, the integrated use of telecommunications and informatics. (Wiley Decl. Ex. A (Doc. No. 219-4, 5) at 1.) His leadership and commitment to community and technology have garnered him many diverse awards, including the National Guard Bureau's Minute-Man-Award in 2006 for providing service and support "above and beyond the call of duty" during the 2005 hurricane season and the 2004 Teleport Developer of the Year Award for Technical Excellence and Innovation. (Fielder Decl. Ex. A. (Doc. No. 219-3) at 1-2.) As the leader of PACid, Mr. Fielder continues to develop his technologies and related products. PACid is an encryption technology research firm, specializing in dynamic key management.

The defendants in this case are Broadcom Corporation, Intel Corporation, Atheros Communications, Inc., Realtek Semiconductor Corporation, and Edimax Technology Co., Ltd.

[1] Exhibits hereto are attached to the Declaration of Stanley H. Thompson, Jr. in Support of Plaintiff The PACid Group, LLC's Opening Brief Regarding Claim Construction, filed concurrently herewith.

(collectively, the "Defendants").

The Patents-in-Suit relate to a system of encryption, and applications thereof, that provide a way to secure the contents of communications in a manner that is highly resistant to attempts to decipher the encoded communications. *See* '646 Patent, 3:18-23; '612 Patent 1:8-14. A consumer's confidence in being able to send communications over the Internet securely, particularly for financial transactions, is fundamental to online commerce. *See, e.g.*, '612:39-45; '646:35-40. Thus, a system that provides for secure communications is highly valuable, and Defendants profit by exploiting the inventions claimed in the Patents-in-Suit.

The proceeding before the Court will construe the disputed terms of the Patents-in-Suit, and thus determine the metes and bounds of PACid's intellectual property.

II. APPLICABLE LEGAL PRINCIPLES

While the Court is clearly familiar with the law as it relates to claim construction, PACid highlights for the Court the overriding legal principles that are relevant to claim construction in this matter. First, a disputed claim term must be considered in the context of the entire claim. *Phillips v. AWH Corp*., 415 F.3d 1303, 1314 (Fed. Cir. 2005) ("To begin with, the context in which a term is used in the asserted claim can be highly instructive."). "It is well settled that, in interpreting an asserted claim, the court should look first to the intrinsic evidence of record, i.e. the patent itself, including the claims, the specification, and, if in evidence, the prosecution history." *Vitronics Corp. v. Conceptronic, Inc*., 90 F.3d 1576, 1582 (Fed. Cir. 1996). Second, the danger of reading limitations from the specific embodiments described in the specification must be avoided. *Phillips*, 415 F.3d at 1319-1320 ("one of the cardinal sins of patent law [is] reading a limitation from the written description into the claims." (quoting *SciMed Life Sys., Inc. v. Advanced Cardiovascular Sys., Inc*., 242 F.3d 1337, 1340 (Fed. Cir. 2001)). Third, the claims should not be construed to exclude a preferred embodiment. *See Chimie v. PPG Indus., Inc.*, 402 F.3d 1371, 1377 (Fed. Cir. 2005) ("[A] construction that would not read on the preferred embodiment would rarely if ever be correct and would require highly persuasive evidentiary

support." (internal quotations and alterations omitted)). Fourth, claim terms should be construed such that dependent claims are more narrow in scope than their related independent claims. *See Nazomi Commc'ns, Inc. v. Arm Holdings, PLC.*, 403 F.3d 1364, 1370 (Fed. Cir. 2005) ("Claim differentiation 'normally means that limitations stated in dependent claims are not to be read into the independent claim from which they depend.'" (quoting *Karlin Tech., Inc. v. Surgical Dynamics, Inc.*, 177 F.3d 968, 971-72 (Fed. Cir. 1999)).

In an apparent attempt to further non-infringement or invalidity defenses, the Defendants' proposed constructions seek to add extraneous limitations to otherwise easily understood terms, exclude disclosed embodiments, and violate other basic principles of claim construction. These constructions are an invitation to error under the aforementioned standard canons of claim construction. The Court should reject them and adopt PACid's proper constructions.

III. UNDISPUTED CLAIM TERMS

The parties have agreed on proposed constructions for certain terms that are identified in the Joint Claim Construction and Prehearing Statement. (Doc. No. 242.) These proposed constructions are incorporated herein by reference.

IV. DISPUTED CLAIM TERMS

A. Pseudo-Random:[2] Apparently Random, But Repeatable And Predictable.

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No construction necessary. If construed: apparently random, but repeatable and predictable.	Refers to output that is repeatable and predictable to anyone who knows the function's inputs but appears to be totally random to those without such knowledge.

PACid contends that this term does not need to be construed because the jury may apply its plain meaning.

[2] "Pseudo-random" appears in Claim 1 of the '646 Patent and Claim 1 of the '612 Patent. The parties agree that it should be construed the same in each patent.

If the term is construed, it should be construed as: "apparently random, but repeatable and predictable." PACid's proposed construction is entirely consistent with the specification. Both the '646 Patent and the '612 Patent state the following: "The term 'pseudo-random' as used in this specification means that the output referred to is repeatable and predictable to anyone who knows the E-Key seed input to the function producing the output. Without such knowledge, the output appears to be totally random." (Ex. A, Col. 5, ll. 14-18; Ex. B, Col. 4, ll. 1-4.)

The specification states that the relevant properties of a pseudo-random output are that it is repeatable and predictable, yet apparently random. These properties, and only these properties, are included in PACid's proposed construction.

Defendants' proposed construction, however, contains at least three instances of surplus language. First, Defendants' inclusion of "to anyone who knows the function's inputs" is unnecessary. It is irrelevant to the meaning of "pseudo-random" that someone knows the input. Second, Defendants' inclusion of "to those without such knowledge" is also unnecessary. It is similarly irrelevant who lacks knowledge of the function's inputs. Third, Defendants' proposal that a "pseudo-random" output appears "*totally* random" as opposed to "random" is unhelpful. It is unclear what distinction, if any, is intended by the inclusion of the term "totally."

Accordingly, PACid respectfully requests that the Court adopt its proposed construction.

B. Constant Value:[3] A Value That Does Not Change For Any Given Instance Of Generating An Encryption Key.

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No construction necessary. If construed: A value that does not change for any given instance of generating an encryption key.	A value that does not change.

PACid's and Defendants' respective proposed constructions for the term "constant value" differ in that PACid's construction is consistent with the teachings of the Patents-in-Suit while Defendants' proposed construction improperly excludes a preferred embodiment.

[3] "Constant value" appears in Claim 1 of the '646 Patent and Claim 1 of the '612 Patent. The parties agree that it should be construed the same in each patent.

> The specification of the '612 Patent describes the constant value as follows:
>
> FIG. 6 shows the various bit fields that could make up a constant value 11. A length byte 50 indicates the total number of bytes in the constant value 11. The length byte is necessary because a number of the remaining bit fields of the constant value are of *variable length*. Following the length byte 50 is the E-Key Seed ID 51 which is used as a table look-up tag associated with the corresponding E-Key Seed stored in an E-Key Seed table. When the constant value 11 is first being formed, the *E-Key Seed ID is automatically entered as that of the host system*. A user is prompted, however, to either accept the ID *or assign another*. In this manner[] files may be shared between PCs, workstations, and workgroups that normally use different E-Key Seeds. The encryption algorithm 52 is *optional* to accommodate communication interoperability between parties that normally use different encryption algorithms.

(Ex. B ('612 Patent), Col. 6, ll. 6-21, Fig. 6 (emphasis added).) This portion of the specification describes examples of a constant value as having several different components that can be changed. For example, a constant value can include an E-Key Seed ID, and the user may choose to assign another E-Key Seed ID. The E-Key Seed ID is described as being that of the host system by default, which implies that it can differ between host systems. Furthermore, the constant value is expressly described as having a variable length, implying that it can have different values with different lengths. Another field used to designate the encryption algorithm is optional. The "constant value" of the claimed invention is not a universal and immutable value that does not change.

A plain reading of the claims of the Patents-in-Suit illustrates that the constant value recited therein only has to be constant for the purpose of generating a given encryption key. Once the encryption key is generated and used according to the claims of the Patents-in-Suit, another constant value may be used to generate a subsequent different encryption key. Defendants' proposed construction that a constant value does not change—period—contradicts

the express teachings of the inventors and excludes a preferred embodiment from Figure 6. This is an invitation to error. *See Chimie*, 402 F.3d at 1377.

Accordingly, PACid's proposed construction should be adopted.

C. Shuffled Bit Result:[4] The Result Of An Algebraic, Cryptographic And/Or Logic Function That Mixes Binary Digits.

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
The result of an operation that mixes the bits of its inputs.	The result of an operation that randomly mixes and maps the bits of its inputs.

PACid proposes that the "shuffled bit result" be construed as: "the result of an operation that mixes the bits of its inputs." PACid's proposed construction is completely consistent with the specification.

The specification of the '646 Patent states that "an E-Key Seed 50 and constant value 51 are combined by a bit-shuffling generator 52 that executes an algebraic, cryptographic and/or logic function, which by way of example but not limitation may be the equation A⊕B=C, where A is the E-Key Seed 50 and B is the constant value 51." (Ex. A, Col. 4, ll. 60-65.) This portion of the specification states that two values are combined and their bits mixed through an algebraic, cryptographic and/or logic function. The specification fully supports PACid's construction.

Defendants' construction, which requires a "random" mix of bits, excludes a preferred embodiment. The specification provides as an example preferred embodiment a bit-shuffling generator that executes the equation A⊕B=C, which is not random. In addition, the specification states that "[t]he result C is a pseudo-random bit sequence … ." (Ex. A, Col. 5, ll. 1-2.) Although the specification also states that "[t]he bits of the E-Key Seed and the constant value thereby are randomly mixed and mapped to a result C of fewer total bits than the combination of the E-Key Seed and the constant value" (Ex. A, Col. 4, l. 65–Col. 5, l. 1), this reference to random mixing does not justify a construction that would appear to preclude the result being a pseudo-random bit sequence, which is expressly disclosed in the specification.

[4] "Shuffled bit result" appears in Claim 1 of the '646 Patent.

Accordingly, PACid's proposed construction should be adopted.

D. Secure Hash Operation:[5] An Algorithm That Produces A Deterministic Output Having No Known Relationship With The Input That May Be Used To Recover The Input From The Output.

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
An algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output.	An operation that can accept an input of variable bit length, but always produces an output having the same bit length such that it is computationally infeasible to determine (a) the input from the output and (b) two inputs that produce the same output, and where if a single bit of the input is changed, approximately 50% of the output bits are changed.

PACid proposes that "secure hash operation" should be construed as: "an algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output." PACid's proposed construction is fully consistent with the specification. Both the '646 Patent and the '612 Patent state the following: "There is no known relationship between the input and output of a hash algorithm which may be used to recover the input from the output." (Ex. A, Col. 2, ll. 8-10; Ex. B, Col. 2, ll. 15-17.)

The specification states that the relevant property of a secure hash function is that there is no known relationship between the input and output of a hash algorithm that may be used to recover the input from the output. This property is expressed in PACid's proposed construction.

Defendants' proposed construction, however, attempts to incorporate the limitations of a single disclosed embodiment. Importing limitations from the specification is improper. *Phillips*, 415 F.3d at 1319-1320. The limitation in Defendants' proposed construction regarding 50% of the bits of the output changing if one bit of the input is changed is taken out of context from the discussion of FIPS PUB 180-1, Secure Hash Standard, a publication disclosed in the specifications of the '646 Patent and the '612 Patent. (Ex. A, Col. 1, l. 58–Col. 2, l. 11; Ex. B, Col. 1, l. 65–Col. 2, l. 18.) One of ordinary skill in the art would not understand "secure hash

[5] "Secure hash operation" appears in Claim 1 of the '646 Patent and Claim 1 of the '612 Patent. The parties agree that it should be construed the same in each patent.

operation" as necessarily having the property of 50% of the bits of the output changing if one bit of the input is changed. Defendants are improperly attempting to incorporate the limitations of a single disclosed embodiment in their proposed construction.

Accordingly, PACid respectfully requests that the Court adopt its proposed construction.

E. Performing A Secure Hash Operation On Said Shuffled Bit Result To Produce A Message Digest:[6] No Separate Construction Required

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No separate construction necessary.	The input to the secure hash operation is the shuffled bit result from step (a), and the output of the secure hash operation is a message digest.

The parties all agree that "secure hash operation" and "shuffled bit result" need to be construed, as discussed above. Defendants have not proposed a separate construction for "message digest." Therefore, PACid proposes that no separate construction is necessary for the term "performing a secure hash operation on said shuffled bit result to produce a message digest" as the jury may apply its plain meaning in light of the construction of "secure hash operation" and "shuffled bit result."

F. Algebraic function:[7] No Construction Necessary

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No construction necessary. If construed: any operation used in mathematics.	Any operation used in mathematics or logic.

PACid contends that this term does not need to be construed because the jury may apply its plain meaning.

If the term is construed, it should be construed as: "any operation used in mathematics." PACid's proposed construction differs from Defendants' in that Defendants' construction includes "or logic" as part of the construction. Defendants' proposed construction is inconsistent

[6] "Performing a secure hash operation on said shuffled bit result to produce a message digest" appears in Claim 1 of the '646 Patent.

[7] "Algebraic function" appears in Claim 1 of the '612 Patent and Claim 3 of the '646 Patent. The parties agree that it should be construed the same in each patent.

with the claims. "Algebraic function" appears in the "combining" step of Claim 1 of the '612 Patent. Claim 4, however, recites "[t]he method of claim 1 wherein said step of combining includes one or more logic functions." (Ex. B, Col. 7, ll. 66-67 (Claim 4).) If an algebraic function included logic functions, as proposed by Defendants, it would render Claim 4 superfluous, which is contrary to the doctrine of claim differentiation. *See Nazomi Commc'ns*, 403 F.3d at 1370. Defendants' proposed construction is also inconsistent with the specifications of the Patents-in-Suit, which discuss both algebraic functions and logic functions, implying that a logic function is not an algebraic function. (*See, e.g.,* Ex. A, Col. 4, l. 62 "an E-Key Seed 50 and constant value 51 are combined by a bit-shuffling generator 52 that executes an algebraic, cryptographic and/or logic function"; Ex. B, Col. 6, l. 53 ("a cleartext constant value and a secret E-Key Seed are combined by one or more logic, encryption and/or algebraic functions").)

Accordingly, PACid respectfully requests that the Court adopt its proposed construction.

G. Host System: A System For Providing Command Sequences.[8]

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No construction necessary. If construed: a system for providing command sequences.	Computer that inputs command sequences to an encryption key generator.

PACid contends that this term does not need to be construed because the jury may apply its plain meaning.

If the term is construed, it should be construed as: "a system for providing command sequences." All parties agree that a host system provides command sequences. For example, the specification of the '646 Patent states that "FIG. 5a shows a command sequence 125 which is issued by the host system to activate the encryption key generator system 100." (Ex. A ('646 Patent), Col. 7, ll. 50-52.) This fully supports PACid's construction of "a system for providing command sequences."

[8] "Host System" appears in Claim 12 of the '646 Patent.

Defendants' proposed construction is inconsistent with the surrounding claim language and is not supported by the specifications of the '646 Patent. Claim 12 expressly recites that an encryption key generator comprises "an I/O interface means in electrical communication with said host system and receiving command sequences from said host system." Accordingly, Defendants' proposed construction is inconsistent with the context of the related claim language. Furthermore, nowhere in the specification of the '646 Patent does it state that the host system is a "computer." This is a limitation inserted without support by Defendants.

Accordingly, PACid respectfully requests that the Court adopt its proposed construction.

H. Interrupt Control Means:[9] Hardware Or Software That Issues A Signal To Interrupt The Operation Of A Processor.

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
This term is not governed by 35 U.S.C. section 112, P. 6, and should given its plain meaning, or alternatively if the Court decides that construction is necessary: "hardware or software that issues a signal to interrupt the operation of a processor" If the Court decides that this phrase is governed by 35 U.S.C. section 112, P. 6: Recited Function: issuing an interrupt signal upon receipt of command sequences Corresponding Structure: interrupt control unit 104	**Function: issuing an interrupt signal upon receipt of said command sequences** **Structure: No corresponding structure; claim is indefinite**

This term should not be interpreted under 35 U.S.C. § 112, ¶ 6. The presumption that a term using the "means for" format should be interpreted under 35 U.S.C. § 112, ¶ 6 is rebutted if the claim recited sufficient structure to perform the claimed function. *See Envirco Corp. v. Clestra Cleanroom, Inc.*, 209 F.3d 1360, 1364 (Fed. Cir. 2000); *see also Sage Prods., Inc. v. Devon Indus., Inc.*, 126 F.3d 1420, 1427-28 (Fed. Cir. 1997) ("Where a claim recites a function, but then goes on to elaborate sufficient structure, material or acts within the claim itself to

[9] "Interrupt control means … for issuing an interrupt signal upon receipt of said command sequences" appears in Claim 12 of the '646 Patent.

perform entirely the recited function, the claim is not in means-plus-function format."). In this case, the presumption is rebutted.

Interrupt controls are well-known in the art of computer architecture. *See, e.g.*, Ex. C, "Interrupt," *The Authoritative Dictionary of IEEE Standards Terms* 583 (7th ed. 2000). The specification describes the operation of the interrupt control unit, reference numeral 104 in Fig. 3. (Ex. A ('646 Patent), Col. 6, l. 43–Col. 7, l. 6 & Fig. 3.) In particular, the specification states that "[w]hen information from the host system is written into the I/O interface unit 102, an interrupt is generated by the interrupt control unit 104." (*Id.*, at Col. 6, l. 66–Col. 7, l. 1.) The interrupt control unit defines a definite structure to one of ordinary skill in the art in the context of the claims and specification. As such, the claim term presented is not subject to 35 U.S.C. § 112, ¶ 6, and should not be construed as such. Instead, it should be construed as "hardware or software that issues a signal to interrupt the operation of a processor."

If this term is construed to be subject to 35 U.S.C. § 112, ¶ 6, it is not indefinite. The recited function is issuing an interrupt signal upon receipt of command sequences. The specification states that the interrupt control unit generates an interrupt when information from the host system is written into the I/O interface unit. (*Id.*, at Col. 6, l. 66–Col. 7, l. 1 & Fig. 3.) As discussed above in connection with the term "host system," the host system provides command sequences to the encryption key generator. (*Id.*, at Col. 7, ll. 50-52.) Thus, the interrupt control unit 104 disclosed the '646 Patent performs all of the functions recited in the claim and is the corresponding structure for the "interrupt control means" even if that term is construed under 35 U.S.C. § 112, ¶ 6.

Accordingly, "interrupt control means" is not subject to 35 U.S.C. § 112, ¶ 6, and should be construed as "hardware or software that issues a signal to interrupt the operation of a processor." However, if "interrupt control means" is construed under 35 U.S.C. § 112, ¶ 6, its corresponding structure is the interrupt control unit 104 described in the specification, and thus the term is not indefinite.

I. Bit-Shuffle Computer Program:[10] No Separate Construction Required, Or Alternatively, "A Computer Program That Mixes The Bits Of Inputs."

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No separate construction necessary due to the construction of "shuffled bit result." If construed: a computer program that mixes the bits of inputs.	Computer program that randomly mixes and maps the bits of its inputs.

The parties agree that "shuffled bit result" needs to be construed, as discussed above. Therefore, PACid proposes that no separate construction is necessary for the term "bit-shuffle computer program" because the jury may apply its plain meaning in light of the construction of "shuffled bit result." If construed, this term should be construed consistently with "shuffled bit result" as "a computer program that mixes the bits of inputs."

J. Secure Hash Computer Program:[11] No Separate Construction Required, Or Alternatively, "A Computer Program That Produces A Deterministic Output Having No Known Relationship With The Input That May Be Used To Recover The Input From The Output."

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No separate construction necessary due to the construction of "secure hash operation." If construed: a computer program that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output.	computer program that uses a secure hash algorithm

The parties all agree that "secure hash operation" needs to be construed, as discussed above. Therefore, PACid proposes that no separate construction is necessary for the term "secure hash computer program" because the jury may apply its plain meaning in light of the construction of "secure hash operation." If construed, this term should be construed consistently with "secure hash operation" as "a computer program that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output."

[10] "Bit-shuffle computer program" appears in Claim 12 of the '646 Patent.

[11] "Secure hash computer program" appears in Claim 12 of the '646 Patent.

K. Secure Hash Algorithm:[12] No Separate Construction Required, Or Alternatively, "An Algorithm That Produces A Deterministic Output Having No Known Relationship With The Input That May Be Used To Recover The Input From The Output.".

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No separate construction necessary due to the construction of "secure hash operation." If construed: an algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output.	An algorithm that can accept an input of variable bit length, but always produces an output having the same bit length such that it is computationally infeasible to determine (a) the input from the output and (b) two inputs that produce the same output, and where if a single bit of the input is changed, approximately 50% of the output bits are changed.

The parties all agree that "secure hash operation" needs to be construed, as discussed above. Therefore, PACid proposes that no separate construction is necessary for the term "secure hash algorithm" because the jury may apply its plain meaning in light of the construction of "secure hash operation." If construed, this term should be construed consistently with "secure hash operation" as "an algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output."

L. Logic Function:[13] No Construction Necessary, Or Alternatively, "A Function Involving Operations On Variables That May Only Take A Finite Number Of Possible Values Or States."

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No construction necessary. If construed: a function involving operations on variables that may only take a finite number of possible values or states.	A function that involves yes-no decisions.

PACid contends that this term does not need to be construed because the jury may apply its plain meaning.

If the term is construed, it should be construed as: "a function involving operations on variables that may only take a finite number of possible values or states." This construction is

[12] "Secure hash algorithm" appears in Claim 12 of the '646 Patent.

[13] "Logic function" appears in Claim 4 of the '612 Patent and Claim 14 of the '646 Patent. The parties agree that it should be construed the same in each patent.

consistent with the specification. The specification of the '646 Patent states that "an E-Key Seed 50 and constant value 51 are combined by a bit-shuffling generator 52 that executes an algebraic, cryptographic and/or logic function, which by way of example but not limitation may be the equation A⊕B=C, where A is the E-Key Seed 50 and B is the constant value 51." (Ex. A, Col. 4, ll. 60-65.) The symbol ⊕ denotes the logic function "exclusive-or" which compares the bits of two inputs and outputs, for example, a "1" if one and only one of the inputs is "1," and otherwise outputs a "0." Alternatively, a logic function can involve the values "true" or "false." In computer systems, variables of a logical function can typically take on one of two values. What is important is that the possible choices of values is finite.

PACid's proposed construction is also consistent with the dictionary definition for "logical operation": "an operation involving logical variables and operators."[14] A "logical variable," also know as a "switching variable," is "a variable that may take only a finite number of possible values or states."[15]

Defendants' proposed construction is defective in that it narrowly proposes that only "yes" or "no" can be the possible results of a logic function. Furthermore, Defendants' proposed construction introduces a confusing uncertainty regarding what is meant by "decisions."

Accordingly, PACid's proposed construction should be adopted.

M. Cryptographic Function:[16] No Construction Required, Or Alternatively, "A Function Used In Encoding Or Decoding."

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No construction necessary. If construed: a function used in encoding or decoding.	A function used in encryption or decryption.

PACid contends that this term does not need to be construed because the jury may apply its plain meaning.

[14] Ex. C, The Authoritative Dictionary of IEEE Standards Terms 637.

[15] Ex. C, The Authoritative Dictionary of IEEE Standards Terms 637.

[16] "Cryptographic function" appears in Claim 15 of the '646 Patent and Claim 5 of the '612 Patent. The parties agree that it should be construed the same in each patent.

If the term is construed, it should be construed as: "a function used in encoding or decoding." This proposed construction is consistent with the dictionary meaning of the word "cryptography": "study of encoding."[17] Defendants' proposed construction imposes unnecessarily narrow limitations that find no support in the specification.

Accordingly, PACid's proposed construction should be adopted.

N. Bit Shuffling Operations:[18] No Separate Construction Required, Or Alternatively, "Operations That Mix The Bits Of Its Inputs."

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No separate construction necessary due to the construction of "shuffled bit result." If construed: operations that mix the bits of their inputs.	operations that randomly mix and map the bits of their inputs.

The parties all agree that "shuffled bit result" needs to be construed, as discussed above. Therefore, PACid proposes that no separate construction is necessary for the term "bit shuffling operations" because the jury may apply its plain meaning in light of the construction of "shuffled bit result." If construed, this term should be construed consistently with "shuffled bit result" as "operations that mix the bits of their inputs."

O. Function To Shuffle Bits/ Bit Shuffling Function:[19] No Separate Construction Required, Or Alternatively, "A Function That Mixes The Bits Of Its Inputs."

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No separate construction necessary due to the construction of "shuffled bit result." If construed: a function that mixes the bits of its inputs.	A function that randomly mixes and maps the bits of its inputs.

The parties all agree that "shuffled bit result" needs to be construed, as discussed above. Therefore, PACid proposes that no separate construction is necessary for the terms "function to

[17] Ex. D, Encarta World English Dictionary 435 (1999).

[18] "Bit shuffling operations" appears in Claim 18 of the '646 Patent.

[19] "Function to shuffling bits" appears in Claim 1 of the '612 Patent. "Bit shuffling function" appears in Claim 19 of the '646 Patent. The parties agree that these terms should be given the same construction.

shuffle bits" and "bit shuffling function" because the jury may apply its plain meaning in light of the construction of "shuffled bit result." If construed, this term should be construed consistently with "shuffled bit result" as "a function that mixes the bits of its inputs."

P. Information File:[20] Message Or File.

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
Message or file.	A collection of information stored as a unit and identified by a unique name.

PACid proposes that the "information file" be construed as: "message or file." PACid's proposed construction is consistent with the specification of the '612 Patent.

The '612 Patent states that it relates to "a method and system for protecting an information file from unauthorized access, and more specifically to the encryption of a *message or file* … ." (Ex. B ('612 Patent), Col. 1, ll. 8-10 (emphasis added).) Furthermore, the '612 Patent states that "[a] method and system is disclosed for protecting sensitive information *files and messages* from access by unauthorized parties … ." (*Id.*, Col. 3, ll. 12-14 (emphasis added).) These disclosures fully support PACid's proposed construction that an "information file" is a "message or file."

Defendants' proposed construction imposes unnecessarily narrow limitations that find no support in the specification. Moreover, a one of ordinary skill in the art would recognize that a computer file may not always be stored as one contiguous unit. Rather, a file can be broken into components linked together by a file management system. Defendants' construction is thus inconsistent with the normal usage of "file" in the patents and the relevant art.

Accordingly, PACid's proposed construction should be adopted.

[20] "Information file" appears in Claim 1 of the '612 Patent.

Q. Performing A Secure Hash Operation On Said First Pseudorandom Result To Effect A Second Many-To-Few Bit Mapping And Produce A Second Pseudo-Random Result:[21] No Separate Construction Required, Or Alternatively, "Performing An Algorithm That Produces A Deterministic Output Having No Known Relationship With The Input That May Be Used To Recover The Input From The Output."

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No separate construction necessary due to the construction of "secure hash operation." If construed: Performing an algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output.	The input to the secure hash operation that effects a second many-to-few bit mapping is the first pseudo-random result from step (a), and the output of the secure hash operation is a second pseudo-random result.

The parties all agree that "secure hash operation" needs to be construed, as discussed above. PACid does not believe that "pseudo-random" needs to be construed, but if it does its construction is not addressed by Defendants' proposed construction. Defendants' also do not propose a construction for "many-to-few bit mapping" as part of their proposed construction for this term. Therefore, PACid proposes that no separate construction is necessary for the phrase "performing a secure hash operation on said first pseudorandom result to effect a second many-to-few bit mapping and produce a second pseudo-random result" the jury may apply its plain meaning in light of the construction of "secure hash operation." If construed, this term should be construed consistently with "secure hash operation" as "performing an algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output."

[21] "Performing a secure hash operation on said first pseudorandom result to effect a second many-to-few bit mapping and produce a second pseudo-random result" appears in Claim 1 of the '612 Patent.

R. Concatenating:[22] Linking Units Together.

PACID'S CONSTRUCTION	DEFENDANTS' CONSTRUCTION
No construction necessary. If construed: linking units together.	Placing one bit field directly next to another.

PACid contends that this term does not need to be construed because the jury may apply its plain meaning.

If the term is construed, PACid proposes that the "concatenating" be construed as: "linking units together." PACid's proposed construction is consistent with the specification of the '612 Patent.

The '612 Patent describes the following: "The encrypted file at the output of processor 30 is concatenated with the constant value 11, and the result is applied to a secure hash function generator 31 to create the message integrity code (MIC) 12 to detect alterations to the encrypted information file." (Ex. B ('912 Patent), Col. 5, ll. 42-46.) The '612 Patent also describes that "[t]he encrypted information file and the constant value then are concatenated to place the constant value in the header at the beginning of the encrypted information file." (Ex. B ('912 Patent), Col. 6, ll. 61-64.) The specification thus describes an encrypted file and a constant value being linked together, which is consistent with PACid's proposed construction. PACid's proposed construction is also consistent with the dictionary definition for "concatenate" as used in computing: "link units together."[23]

Defendants' proposed construction would limit the construction to an embodiment shown in the specification, even though the term is broader than the particular application shown. Restricting a claim term to the manner it is used in a preferred embodiment is incorrect: "Even when the specification describes only a single embodiment, the claims of the patent will not be read restrictively unless the patentee has demonstrated a clear intention to limit the claim scope

[22] "Concatenating" appears in Claim 1 of the '612 Patent.

[23] Ex. D, Encarta World English Dictionary 374 (1999).

using 'words or expressions of manifest exclusion or restriction.'" *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 906 (Fed. Cir. 2004).

Accordingly, PACid's proposed construction should be adopted.

V. CONCLUSION

PACid's proposed constructions are solidly based on intrinsic evidence, and are appropriately consistent with extrinsic evidence. In contrast, Defendants' proposed constructions improperly seek to import unwarranted limitations into the claims, exclude preferred embodiments, and violate the basic structure of the dependent claims. For all of the foregoing reasons, PACid respectfully submits that its proposed constructions and proffered meanings be adopted by this Court.

Dated: February 19. 2010

Respectfully submitted,

By: /s/ Stanley H. Thompson, Jr.
Marc A. Fenster, CA Bar # 181067
Email: mfenster@raklaw.com
Stanley H. Thompson, Jr., CA Bar # 198825
Email: sthompson@raklaw.com
Alexander C. Giza, CA Bar # 212327
Email: agiza@raklaw.com
Andrew D. Weiss, CA Bar # 232974
Email: aweiss@raklaw.com
RUSS, AUGUST & KABAT
12424 Wilshire Blvd., 12th Floor
Los Angeles, California 90025
Telephone: 310/826-7474
Facsimile: 310/826-6991

Andrew W. Spangler, TX Bar # 24041960
Email: spangler@spanglerlawpc.com
LEAD COUNSEL
SPANGLER LAW P.C.
208 N. Green Street, Suite 300
Longview, Texas 75601
Telephone: 903/753-9300
Facsimile: 903/553-0403

Debera W. Hepburn, TX Bar # 24049568
Email: dhepburn@heplaw.com
HEPBURN LAW FIRM PLLC
P.O. Box 118218
Carrollton, TX 75011

Telephone: 214/403-4882
Facsimile: 888/205-8791

Elizabeth A. Wiley, TX Bar # 00788666
THE WILEY FIRM, PC
Email: lizwiley@wileyfirmpc.com
P.O. Box. 303280
Austin, Texas 78703-3280
Telephone: 512/420-2387
Facsimile: 512/551-0028

Robert P. Kelly, MI SB # P72574
E-mail: Robert@robertpkellypllc.com
ROBERT P. KELLY PLLC
938 Chester
Birmingham, MI 48009
Telephone: 248/703-8760
Facsimile: 248/251-0267

Attorneys for Plaintiff
PACID, LLC

CERTIFICATE OF SERVICE

I hereby certify that the following counsel of record who are deemed to have consented to electronic service are being served on February 19, 2010, with a copy of this document via the Court's CM/ECF system. Any other counsel of record will be served by first class U.S. mail on this same date.

By: /s/ Stanley H. Thompson, Jr.
Stanley H. Thompson, Jr.